Cross-Border Access to Electronic Evidence: Solutions for a European Approach

27th September 2018
European Parliament, ASP 4F 384

EuroISPA

E-Evidence Proposal

Dr. Maximilian Schubert LL.M

Vice President, Chair Cybersecurity Committee, EuroISPA
General Secretary, ISPA Austria

Agenda

About EuroISPA

Current Concerns

Challenges in Respect to Real Time Interception

EuroISPA: The Voice of ISPs in Europe

- Established in 1997
- The world's largest association of Internet Service Providers (ISPs), representing over 2.500 ISPs across the EU and EFTA countries
- Representing many SME-ISPs
- Reflects the views of ISPs of all sizes from across its member base

Agenda

About EuroISPA

Current Concerns

Challenges in Respect to Real Time Interception

E-Evidence Proposal: Current Concerns

- Privatisation of law enforcement
  - ISPs should not be the actors responsible for verifying the legitimacy of an order
  - Such a task should remain with judicial authorities
- Legislative asymmetries
  - Clarity with regards to principle of double criminality required
  - Significant disparity across Member States for crimes entailing a three-years sentence
- Obstacles for SMEs
  - Lack in adaptability provisions for SMEs
  - Time frames: SMEs do not run 24/7 services
  - Greater administrative burden would cause market disadvantage

EuroISPA

E-Evidence Proposal: Current Concerns

- **Fragmentation of data categorisation**
  - Differentiation between access and transaction data not in line with E-Privacy Regulation
  - Additional burden for ISPs in compliance process
- **Coherence with international standards**
  - Data transfers to LEAs in third-countries should be in line with international standards (i.e. Budapest Convention)
- **Protection of encrypted data**
  - Clarification needed that ISPs are not required to decrypt data
  - Transfer of encrypted data bears risk that more data is handed over than necessary

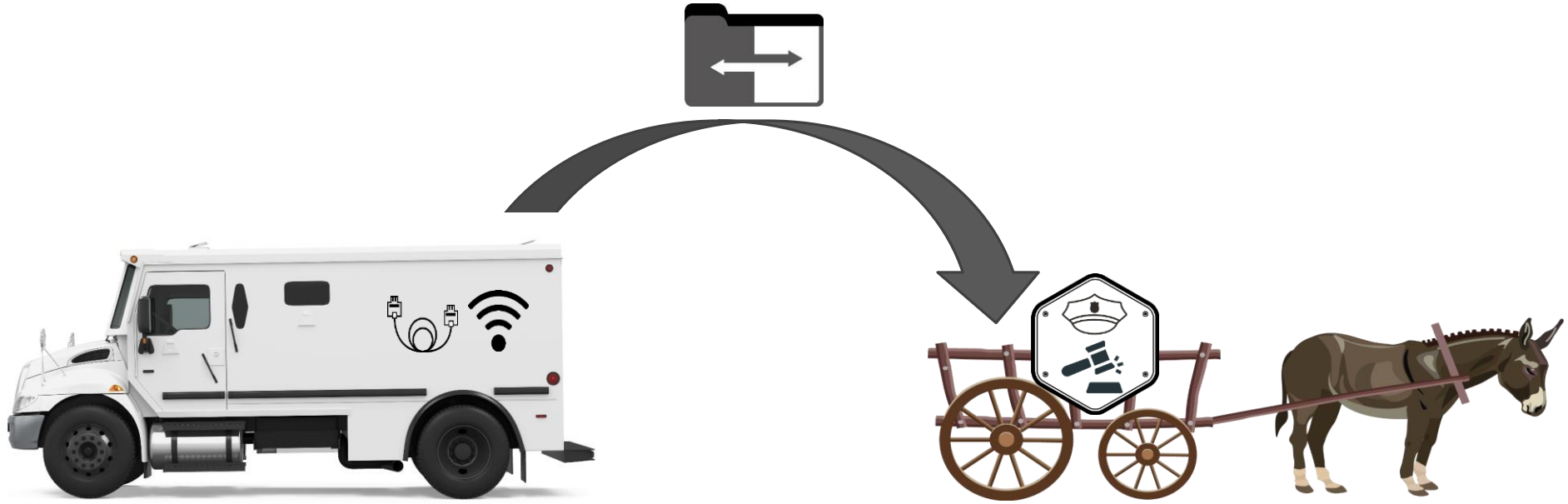
EuroISPA

E-Evidence Proposal: Current Concerns

- Transparency
  - Proposal lacks an enforcement mechanism securing the provision of statistics on issued orders
  - ISPs should be free to publish voluntary transparency reports
- Insufficient authentication of Order Certificates
  - ISPs unable to verify the authenticity of each national judicial authorities' stamp and signature
  - Conditions for security and integrity in executing a Production Order (data transfer)
  - Reservations against downgrading existing information exchange routines to e.g. fax transmissions
- Danger of weakening the high level of security, integrity and trust

EuroISPA

Maintaining an EU-wide high level of transparency and security



Agenda

About EuroISPA

Current Concerns

Challenges in Respect to Real Time Interception

‘Request for information’ ≠ ‘Lawful Interception‘

- Requests for information refer to past access to data retained by ISPs
  - Contract data, traffic data (particularly IP-addresses)
  - Formal procedural requirements
  - Secure data transfer methods (DLS)

- Lawful (Real Time) Interception requests refer to future surveillance of a user’s communication
  - Includes communication content
  - Permitted only for the prosecution of certain crimes
  - Call Content and Interception-related data (IRI) are transferred via highly secure interfaces

EuroISPA

LI: ISP Internal Workflow

- Public prosecutor sends judicially approved order to ISP
- *Formal* review of the request
  (i.e. legitimisation of requesting authority, formal criteria)
- *Legal* review of the request (i.e. check of legal requirements)
- *Contextual* review of the request
  - Identification of user in the operator‘s network (MSISDN, IMSI, IMEI)
  - Duration of surveillance
  - Scope of data concerned

EuroISPA

LI: ISP Internal Workflow

- Contact with public prosecutor to clarify ambiguities if necessary
- Set up and maintenance of the lawful interception method
  - Optional: extension or prolongation
- Internal documentation of the process
- Request for cost reimbursement

LI: ISP Internal Workflow

- Contact with public prosecutor to clarify ambiguities if necessary
- Set up and maintenance of the lawful interception method
- [illegible]
- Internal documentation of the process
- Request for cost reimbursement

EuroISPA

LI: Technical Challenges

- Domestic Lawful Interception (LI) capability requirements are based on different standards (ETSI, 3GPP, ...)
  - Concerns Handover Interfaces (HI) as well as network requirements
- Divergent security requirements regarding the transmission of data (i.e. Cryptoboxes, SINA, ...)
- Transmission of IP-based communication via broadband

EuroISPA

LI: Technical Challenges

- Design of a LI Management system compatible with each Monitoring Center
- Connection to each LEA‘s Monitoring Center (MC) via a Virtual Private Network (VPN)
- Simultaneous transmission of content to several MCs is technically not feasible (concurrent sessions)
- Troubleshooting (raw records)
- After each technical upgrade additional tests with MCs required

Thank You!

EuroISPA
European Internet Services Providers Association
Rue de la Loi 38- 1000 Brussels
T: +32 (0)2 550 41 22
www.euroispa.org

EU Transparency Register No. 54437813115-56

Dr. Maximilian Schubert, General Secretary
ISPA - Internet Service Providers Austria
Währinger Straße 3/18 - 1090 Vienna
T: +43 1 409 55 76

Email maximilian.schubert@ispa.at
Web www.ispa.at

EU Transparency Register No. 56028372438-43

BACKUP

Austrian Example for Safe DataTransfer between LEAs and ISPs: ‘DLS’